

ELEKTRONICZNA WYMIANA DANYCH

Wyciek danych. Jeden atak może uruchomić lawinę kolejnych

Wyciek danych z platformy MyDr, popularnego systemu do fakturowania, i serwisu Wakacje.pl pokazuje, że konsekwencje cyberataku mogą wykraczać daleko poza zaatakowany serwis. Informacje o firmach i ich kontrahentach, dane z faktur, numery rachunków bankowych czy dane dostępne mogą posłużyć do przygotowania kolejnych, trudniejszych do wykrycia oszustw.

Nazwa firmy, NIP, adres, kwota na fakturze czy numer rachunku to z pozoru zwyczajne informacje. W niepowołanych rękach mogą jednak stać się podstawą wiarygodnego scenariusza wyludzenia. Przestępcy mogą wysyłać fałszywe faktury, informować o rzekomej zmianie numeru konta lub podszywać się pod kontrahentów. Znajomość rzeczywistych kwot, numerów dokumen-

tów i historii współpracy sprawia, że takie wiadomości trudniej odróżnić od autentycznej korespondencji.

Zmiana rachunku wymaga weryfikacji

Jednym z zagrożeń po wycieku danych jest oszustwo polegające na podmianie numeru rachunku bankowego na fakturze. Dokument może wyglądać jak oryginał, a je-

dyną zmianą będzie numer konta. Dlatego każda informacja o zmianie danych do płatności powinna uruchamiać dodatkową procedurę bezpieczeństwa. Najlepiej potwierdzić ją telefonicznie, korzystając z numeru znanego wcześniej, a nie danych podanych w otrzymanej wiadomości.

Problem dotyczy również firm korzystających z zewnętrznych systemów księgowych, CRM-ów, platform kadrowych i narzędzi do fakturowania. Nawet dobrze zabezpieczona organizacja może zostać dotknięta incydem u dostawcy. Bezpieczeństwo partnerów technologicznych powinno więc stanowić element zarządzania ryzykiem. Powierzenie danych zewnętrznej firmie nie oznacza automatycznego przeniesienia całej odpowiedzialności za ich ochronę.

Hasło to dopiero początek

Po ujawnieniu informacji o wycieku warto zmienić hasło do zaatakowanego serwisu, a także do powiązanej skrzynki e-mail, jeśli używano tych samych danych logowania. Należy włączyć uwierzytelnianie dwuskładowe, sprawdzić aktywne sesje i listę użytkowników mających dostęp do konta, a także zweryfikować integracje oraz klucze API. Istotne jest również sprawdzenie danych firmy i numerów rachunków na dokumentach oraz poinformowanie pracowników odpowiedzialnych za księgowość i płatności.

Jak podkreśla autorka:

– Wyciek danych może działać w dwóch kierunkach. Firma może otrzymać fałszywą fakturę wystawioną rzekomo przez swojego dostawcę, ale jej własny kontrahent może

również otrzymać wiadomość przygotowaną przez oszusta na podstawie danych dotyczących jego firmy. Dlatego warto uprzedzić najważniejszych partnerów biznesowych, że numer rachunku bankowego pozostaje bez zmian i że każdą wiadomość dotyczącą zmiany danych do płatności należy dodatkowo zweryfikować. Krótka informacja wysłana do kontrahentów może być dziś jednym z prostszych działań ograniczających ryzyko. Warto powiedzieć wprost: jeżeli otrzymacie wiadomość o zmianie naszego rachunku, prosimy o potwierdzenie jej telefonicznie. Nie chodzi o wzbudzanie paniki, tylko o stworzenie dodatkowego punktu kontroli tam, gdzie potencjalny oszust może próbować wykorzystać wyciek – mówi Karolina Praszek-Golebiewska, dyrektor zarządzająca, CEO w Kancelarii Bezpieczeństwa.

REKLAMA

editel

Jeden punkt dostępu.

Połączymy Cię z kontrahentami.

Zanim Twój produkt trafi do Rossmanna, Żabki, Lidl'a czy do innych sklepów, dokumenty muszą spełnić wymagania EDI oraz ViDA.

EDITEL wie, jak to zrobić.

Peppol Access Point

Krajowe Systemy e-Fakturowania

Automotive

Sieci FMCG

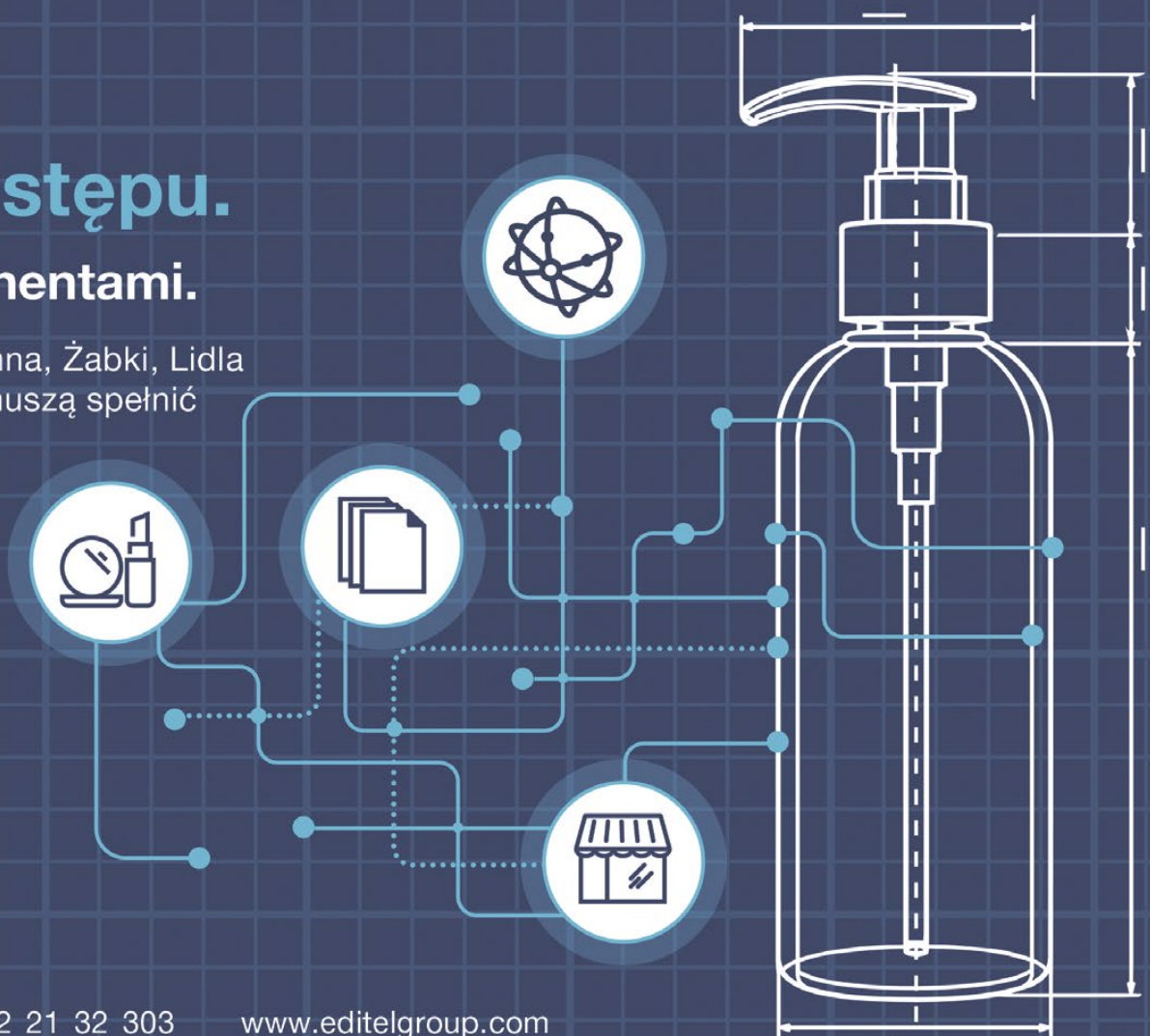
i inne branże

EDITEL S.A.

connect@editelgroup.com

+48 12 21 32 303

www.editelgroup.com



Cyberbezpieczeństwo pod lupą UE

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opublikowała raport ENISA NIS360, który przedstawia ocenę odporności kluczowych sektorów na cyberzagrożenia. W strefie ryzyka znajdują się między innymi ochrona zdrowia, firmy zajmujące się zarządzaniem usługami ICT (technologiami informacyjnymi i komunikacyjnymi) oraz administracja publiczna¹.

SEBASTIAN JAWORSKI
wiceprezes

TOMASZ DZIEDZIC
chief technology officer

MAREK NAJMAJER
product director w Linux Polska

Ostatni z sektorów jest głównym celem cyberataków, co w dużym stopniu wynika z niestabilnej sytuacji geopolitycznej. Ponad 63 proc. działań hakerów (cyberprzestępców motywowanych ideologicznie) na terenie UE jest wymierzonych w podmioty z tego obszaru².

Które sektory wyznaczają standardy w cyberbezpieczeństwie? Agencja opracowała analizę sektorów objętych dyrektywą NIS2, biorąc pod uwagę dwa kluczowe czynniki: krytyczności oraz dojrzałości. Pierwszy z nich obejmuje między innymi poziom cyfryzacji oraz wpływ incydentów na otoczenie społeczno-gospodarcze. W drugim uwzględniono z kolei poziom wsparcia i nadzoru przez odpowiednie organy, zarządzanie ryzykiem cyberbezpieczeństwa, stopień wymiany informacji o zagrożeniach w obrębie sektora oraz gotowość operacyjną do oceny bezpieczeństwa i planowania ciągłości działania³.

Sektor bankowy, energetyczny i telekomunikacyjny ponownie wyróżniają się najwyższym poziomem dojrzałości w zakresie cyberbezpieczeństwa – podobnie jak w ubiegłorocznym badaniu⁴. Jest to po części efekt wymagań regulacyjnych stawianych organizacjom z tych obszarów. Branże z najwyższą oceną w zakresie cyberodporności wyróżniają się większym zaangażowaniem kadry kierowniczej w działania związane z zarządzaniem ryzykiem oraz wyższym

poziomem kompetencji z tego zakresu. Wynika to z kultury organizacyjnej, będącej efektem licznych regulacji prawnych. Przykładowo: w sektorze finansowym jest to rozporządzenie DORA, które nakłada na instytucje ściśle określone wymogi z zakresu bezpieczeństwa IT.

Największa wyzwania stoją przed administracją publiczną
Poziom cyberbezpieczeństwa nie we wszystkich sektorach jest równie wysoki – ENISA wyróżniła kilka z nich w tzw. strefie ryzyka. Oznacza ona niższą dojrzałość w zakresie cyberbezpieczeństwa przy jednoczesnym wysokim poziomie krytyczności. W grupie tej znalazły się transport morski i kolejowy, ochrona

na zdrowia, sektor zarządzania usługami ICT oraz administracja publiczna⁵. Ostatni z wymienionych obszarów charakteryzuje się szczególnie niskim poziomem postępów w zakresie gotowości operacyjnej do zmian w zakresie bezpieczeństwa IT – mimo że jest najbardziej narażony na cyberataki.

Sektor ten wymaga gruntownej zmiany strategii w zakresie zapobiegania ryzyku. Dane ENISA pokazują, że w administracji publicznej problemem nie jest wyłącznie samo wykrywanie podatności. Wiele instytucji potrafi identyfikować je stosunkowo szybko, ale proces usuwania problemów i wdrażania poprawek często trwa trzy miesiące lub dłużej z powodu ograniczonych zasobów. W praktyce oznacza to, że luka między rozpoznaniem ryzyka a jego realnym ograniczeniem pozostaje zbyt duża. Dodatkowym problemem jest brak jasnej hierarchii podatności. W nawale zgłoszeń, formalnych akceptacji i aktualizacji dotyczących drobnych problemów łatwo stracić z pola widzenia te podatności, które

faktycznie mogą zagrozić ciągłości działania usług publicznych. Dlatego administracja potrzebuje przejścia od reaktywnego utrzymania IT do modelu opartego na obserwowalności: stałym zbieraniu i korelowaniu logów, metryk, zdarzeń oraz informacji o zależnościach między systemami. Dopiero wtedy organizacja widzi nie tylko pojedynczy alert techniczny, ale także jego wpływ na konkretną usługę publiczną, priorytet reakcji i źródłową przyczynę problemu.

W praktyce oznacza to odejście od punktowego monitorowania serwerów czy aplikacji na rzecz

widoczności całego łańcucha świadczenia usługi: infrastruktury, aplikacji, baz danych, integracji, sieci, tożsamości użytkowników i dostawców zewnętrznych. Dla instytucji publicznych ma to szczególne znaczenie, ponieważ incydent techniczny bardzo szybko staje się incydem usługowym – utrudnia dostęp do spraw urzędowych, świadczeń, rejestrów lub komunikacji z obywatelami.

Co wpływa na niższą odporność administracji w zakresie bezpieczeństwa?

Dla sektora publicznego największym wyzwaniem w budowaniu cyberodporności jest szybko zmieniający się krajobraz zagrożeń oraz rozwój technologii – w badaniach z 2026 r. odpowiedź tę wskazało 67 proc. podmiotów. Sporym problemem jest także brak kompetencji z tego obszaru, który pozostaje bolączką dla aż 57 proc. organizacji sektora publicznego – to o 19 punktów procentowych więcej niż w przypadku firm prywatnych⁶. ENISA podkreśla jeszcze jeden aspekt. Dyrektywa NIS2, której



Sektor bankowy, energetyczny i telekomunikacyjny wyróżniają się najwyższym poziomem dojrzałości w zakresie cyberbezpieczeństwa.





Sektor administracji publicznej charakteryzuje się najniższym poziomem zaawansowania kadry zarządzającej oraz kompetencji w zakresie cyberbezpieczeństwa.

celem jest podniesienie poziomu cyberbezpieczeństwa w Unii Europejskiej, obejmuje przede wszystkim organy szczebla centralnego, na przykład ministerstwa, urzędy i agencje państwowe. W zależności od kraju jest to szacunkowo od stu do kilku tysięcy instytucji⁷. Problem pojawia się jednak na poziomie regionalnym i lokalnym.

Według analiz ENISA sektor administracji publicznej charakteryzuje się najniższym poziomem zaawansowania kadry zarządzającej oraz kompetencji w zakresie cyberbezpieczeństwa. Co trzecia organizacja nie posiada strategii rozwoju kompetencji z tego zakresu, a połowa nie zapewnia szkoleń dotyczących zagrożeń i analizy ryzyka⁸. Poza ograniczeniami finansowymi i kadrowymi, problemem jest również kultura organizacyjna. Jednostki publiczne cechują się dużym poziomem biurokracji. Przywiązanie do istniejących procedur i technologii często skutkuje niechęcią do wdrożenia nowoczesnych rozwiązań, również z obszaru cyberbezpieczeństwa. Jest to szczególnie widoczne na poziomie gmin i powiatów.

Dodatkową barierą są także opóźnienia we wdrożeniu dyrektywy NIS2, z którymi mierzy się wiele krajów członkowskich UE. Jeszcze w maju ubiegłego roku Komisja Europejska wyśtosowała opinie do 19 państw członkowskich, które nie wdrożyły w pełni dyrektywy NIS2⁸. Wśród nich była również Polska. Sytuacja jednak stopniowo się zmienia. W kwietniu tego roku weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC),

która implementuje unijne regulacje do polskiego porządku prawnego.

Nowe przepisy zobowiązują podmioty objęte dyrektywą NIS do dokonania wpisu do Wykazu KSC do 3 października albo w przypadku samorejestracji

– złożyć wniosek o wpis. Termin wdrożenia wymogów wynikających z nowych przepisów to 3 kwietnia 2027 r. Do tego czasu organizacje będą musiały, m.in. wyznaczyć osoby odpowiedzialne za kontakt z KSC, zweryfikować niekaralność zespołu oraz przygotować i wdrożyć System

Zarządzania Bezpieczeństwem Informacji (SZBI), czyli zestaw polityk, procedur oraz zabezpieczeń organizacyjnych i technicznych minimalizujących ryzyko nieuprawnionego dostępu do danych.

1. ENISA, 2026, ENISA NIS360

2. ENISA, ENISA Threat Landscape 2025

3. Jak wyżej

4. Jak wyżej

5. Jak wyżej

6. World Economic Forum, Global Cybersecurity Outlook 2026.

7. ENISA, 2026, ENISA NIS360

8. Komisja Europejska, Transpozycja dyrektywy NIS 2 w państwach UE

AI zmienia elektroniczny obieg dokumentów. Samo „cyfrowe” już nie wystarczy.

Przez lata elektroniczny obieg dokumentów kojarzył się przede wszystkim z przeniesieniem papierowych procesów do systemu: rejestracją dokumentu, przekazaniem go do odpowiedniej osoby, akceptacją i archiwizacją. Dziś taki model przestaje wystarczać. Firmy nie potrzebują już wyłącznie cyfrowego repozytorium. Potrzebują narzędzi, które potrafią zrozumieć informacje zapisane w dokumentach i wykorzystać je do dalszej automatyzacji procesów.

Właśnie dlatego sztuczna inteligencja staje się jednym z najważniejszych kierunków rozwoju systemów EOD. Dokument coraz rzadziej powinien być traktowany jako plik, który człowiek musi otworzyć, przeczytać i ręcznie opisać. Powinien stać się źródłem ustrukturyzowanych danych, które mogą automatycznie zasilać kolejne etapy procesu.

– Przyszłość elektronicznego obiegu dokumentów nie polega na tym, żeby szybciej przesyłać pliki pomiędzy użytkownikami. Kluczowe jest to, żeby system potrafił zrozumieć, z jakim dokumentem ma do czynienia, jakie informacje są w nim istotne i co powinno wydarzyć się dalej – mówi **Filip Kolendo**, CTO i wiceprezes Primesoft Polska.



Od cyfrowego dokumentu do danych, które pracują

Taką zmianę dobrze widać na przykładzie inteligentnego przetwarzania dokumentów, czyli IDP. Rozwiązania tej klasy łączą OCR z mechanizmami AI oraz przetwarzaniem języka naturalnego. W praktyce oznacza to przejście od prostego rozpoznania tekstu do analizy jego znaczenia.

W systemie V-Desk AI może m.in. identyfikować i klasyfikować typ dokumentu, wyodrębniać kluczowe dane, oceniać ich kompletność, interpretować kontekst, tworzyć podsumowania oraz automatycznie zasilać workflow. Może także analizować informacje zapisane w tabelach, diagramach czy dokumentach w różnych językach. W obiegu korespondencji sztuczna inteligencja może rozpoznać charakter pisma i skierować je do właściwego procesu, np. reklamację do działu jakości, a wezwanie do zapłaty do windykacji.



– Największa wartość AI pojawia się wtedy, gdy przestaje być dodatkiem do systemu, a staje się elementem procesu. Jeżeli po rozpoznaniu dokumentu dane trafiają bezpośrednio do odpowiedniego rejestru, systemu ERP, CRM czy kolejnego kroku workflow, eliminujemy nie tylko ręczne przepisywanie informacji, ale również znaczną część pracy związanej z ich interpretacją – podkreśla Filip Kolendo.

AI jako część procesu, nie dodatek do systemu

To właśnie ten aspekt będzie decydował o konkurencyjności systemów EOD w kolejnych latach. Organizacje przetwarzają coraz większe wolumeny informacji: faktury, umowy, korespondencję, formularze, dokumenty przewoźne, dokumentację HR czy pisma urzędowe. Im więcej danych, tym mniej efektywny staje się model oparty na ręcznej obsłudze. AI może w tym przypadku pełnić rolę pierwszej warstwy analitycznej, o ile będzie potrafiło poprawnie odczytać

dokument, zrozumieć jego kontekst, wskazać braki, wydobyć najważniejsze informacje i przygotować dane do dalszego wykorzystania. Człowiek pozostaje odpowiedzialny za decyzję tam, gdzie jest ona rzeczywiście potrzebna, ale nie musi wykonywać każdej czynności technicznej prowadzącej do jej podjęcia.

– Dojrzały system EOD nie powinien już tylko odpowiadać na pytanie: „Gdzie znajduje się dokument?”. Powinien również odpowiadać: „Co z niego wynika i co należy z nim zrobić?”. Sztuczna inteligencja daje dziś technologiczną możliwość, żeby właśnie w tę stronę rozwijać elektroniczną wymianę danych w przedsiębiorstwach – podsumowuje Filip Kolendo.

Dlatego przyszłość EOD należy nie do systemów, które wyłącznie digitalizują dokumenty, lecz do platform, które zamieniają ich treść w dane, a dane w automatyczne działania. AI nie zastępuje elektronicznego obiegu dokumentów. Staje się jego naturalnym kolejnym etapem.

materiał partnera



AI w cyberbezpieczeństwie po stronie ataku i obrony

Dobrze napisana wiadomość z prośbą o zmianę rachunku do płatności może być próbą oszustwa. Generatywna AI ułatwia przygotowanie takiego tekstu, poprawia język, dopasowuje ton i pozwala szybko tworzyć kolejne wersje. Zespołom bezpieczeństwa pomaga z kolei analizować podejrzane zdarzenia. O wyniku decyduje jednak także to, czy firma potrafi zweryfikować dyspozycję, ograniczyć dostęp napastnika i odtworzyć usługi po incydencie.



ALBERT SZCZEPANIAK
dyrektor Działu Bezpieczeństwa
i Jakości w Polcom

Szybsze przygotowanie ataku Phishing i kradzież danych nie zaczęły się wraz z upowszechnieniem AI. Zmieniają się natomiast czas i nakład pracy potrzebne do przygotowania części ataków. Modele mogą wspierać rozpoznanie celu, analizę podatności i tworzenie kodu. Brytyjskie NCSC wskazuje, że AI zwiększa możliwości atakujących, ale skuteczność zależy od zadania, środowiska i sposobu użycia narzędzia. Automatyzacja poszczególnych etapów nie oznacza, że każdy złożony atak

można niezawodnie przeprowadzić bez udziału człowieka. Większa liczba prób obciąża obrońców. Nie znaczy to jednak, że pojedyncze przeoczenie musi przesądzić o utracie danych. Kontrola uprawnień, podział sieci na strefy i szybkie odizolowanie przejętego urządzenia mogą ograniczyć dalszy przebieg ataku. Firma powinna przygotować się również na sytuację, w której pierwsza warstwa zabezpieczeń zawiedzie. W przemyśle, energetyce czy transporcie trzeba przy tym uwzględnić wpływ incydentu na działanie urządzeń i dostępność usług.

Co AI wnosi do pracy zespołu bezpieczeństwa

Pod nazwą AI kryją się różne metody. Uczenie maszynowe jest od lat wykorzystywane do rozpoznawania podejrzanych wzorców. Modele generatywne mogą natomiast pomagać anali-

tykom w porządkowaniu informacji o incydencie, interpretowaniu logów i przygotowaniu podsumowania. Nie każda automatyczna reakcja ani korelacja zdarzeń wymaga jednak AI.

Warto też rozróżnić SOC i XDR. Security Operations Center to zespół i zorganizowana funkcja monitorowania bezpieczeństwa oraz obsługi incydentów, realizowana wewnętrznie lub przez dostawcę usługi. XDR jest rozwiązaniem technologicznym, które łączy dane o zagrożeniach z różnych źródeł i wspiera wykrywanie oraz reakcję. Może być jednym z narzędzi używanych przez SOC. Praktyczny przykład to analiza nietypowego logowania. Sam adres IP nie rozstrzyga, czy doszło do włamania. Trzeba sprawdzić urządzenie, historię aktywności konta i operacje wykonane po zalogowaniu. Narzędzie może zebrać te informacje i wskazać zależność. Analityk powinien mieć możliwość sprawdzenia, z jakich zdarzeń wynika wniosek.

Odpowiedź modelu językowego może brzmieć przekonująco mimo błędu. Dlatego automatyczne odłączenie systemu produkcyjnego wymaga innych warunków niż przygotowanie roboczego opisu alertu. Zakres samodzielnych działań narzędzia trzeba ustalić z wyprzedzeniem,

wraz z zasadami zatwierdzania i możliwością cofnięcia zmian. Błędna reakcja może sama spowodować przestój.

Dane i integracja przed kolejnym wdrożeniem

W badaniu Polcom „Barometr cyfrowej transformacji polskiego biznesu 2025-2026” 91 proc. badanych firm deklarowało korzystanie z technologii cyberbezpieczeństwa i monitoringu infrastruktury, a 72 proc. wskazywało integrację nowych rozwiązań z istniejącymi systemami jako wyzwanie. Badanie przeprowadzono w kwietniu 2025 roku wśród 100 średnich i dużych przedsiębiorstw. To deklaracje uczestników, a nie pomiar skuteczności ich zabezpieczeń. Przed wdrożeniem AI warto więc sprawdzić, czy zespół otrzymuje logi z najważniejszych systemów, czy zdarzenia mają poprawne znaczniki czasu i czy wiadomo, kto od-

powiada za obsługę alertów. Brak danych z krytycznej aplikacji pozostanie luką w monitoringu, nawet jeśli pozostałe informacje będzie analizował zaawansowany model.

Ochrony wymaga także samo rozwiązanie AI. W systemach korzystających z modeli językowych zagrożeniem jest między innymi prompt injection, np. złośliwa treść, która w analizowanym dokumencie, może próbować nakłonić model do wykonania niepożądanych poleceń. Ryzyko rośnie, gdy model ma dostęp do narzędzi wykonujących operacje w firmowych systemach. Należy ograniczyć jego uprawnienia i kontrolować dane przekazywane do usługi. NIST opisuje również zatrzymywanie danych i ataki na poufność informacji przetwarzanych przez modele.

Odtworzenie usług trzeba przećwiczyć

Nawet sprawna detekcja nie gwarantuje nieprzerwanego działania firmy. Plan odtworzenia środowiska powinien określać kolejność uruchamiania usług, dopuszczalny czas przestoju i akceptowalną utratę ostatnich zmian w danych. Potrzebne są też kopie zapasowe chronione przed przejęciem lub zniszczeniem przez napastnika oraz regularne próby odtwarzania. CISA zaleca między innymi kopie offline i sprawdzanie ich dostępności oraz integralności w scenariuszu awaryjnym.

Zapasowy ośrodek przetwarzania może pomóc przywrócić usługi, lecz sama replikacja danych nie wystarcza do ochrony przed ransomware. Może przenieść do drugiego środowiska również skutki niepożądanych zmian. O użyteczności planu świadczy udana próba odtworzenia, z uwzględnieniem zależności między aplikacjami i kontroli bezpieczeństwa przywracanego środowiska.

Wdrożenie AI warto rozliczać z takich samych konkretów, tj. czasu obsługi incydentu, liczby błędnych alarmów i skutków automatycznych działań. Jeśli analityk szybciej ustala, co się wydarzyło, a firma potrafi bezpiecznie ograniczyć incydent, narzędzie spełnia swoją rolę. Samo oznaczenie produktu jako „AI” niczego jeszcze nie rozstrzyga.



Firma powinna przygotować się na sytuację, w której pierwsza warstwa zabezpieczeń zawiedzie.